ADDENDUM 4 TO APPENDIX 3 TO SCHEDULE 3.3 TO THE COMPREHENSIVE INFRASTRUCTURE AGREEMENT

STATEMENT OF TECHNICAL APPROACH

Statement of Technical Approach for Security Services

The Security Services technical approach is focused on the personnel, systems and security necessary to protect the Commonwealth. Northrop Grumman will visit multiple locations and meet the personnel doing security work. Northrop Grumman will conduct analysis of the currently deployed systems, configurations and policies to complete our proposed solution plan.

After data gathering, Northrop Grumman's technology solution and transition plan will be finalized to enter the approval cycle. Northrop Grumman's security leadership will work closely with the VITA Security Directorate by conducting regular security working group meetings where design, development, integration, and testing will be primary topics. This working group will be the approval entity for the security systems. Northrop Grumman's security engineers and analysts shall provide the appropriate protection levels for confidentiality, availability, and integrity to meet specific policy and direction according to respective executive branch agency.

The VITA IT security workflow depicted in **Exhibit 1** is a summation of the processes relevant to Northrop Grumman's proposed awareness methodology.

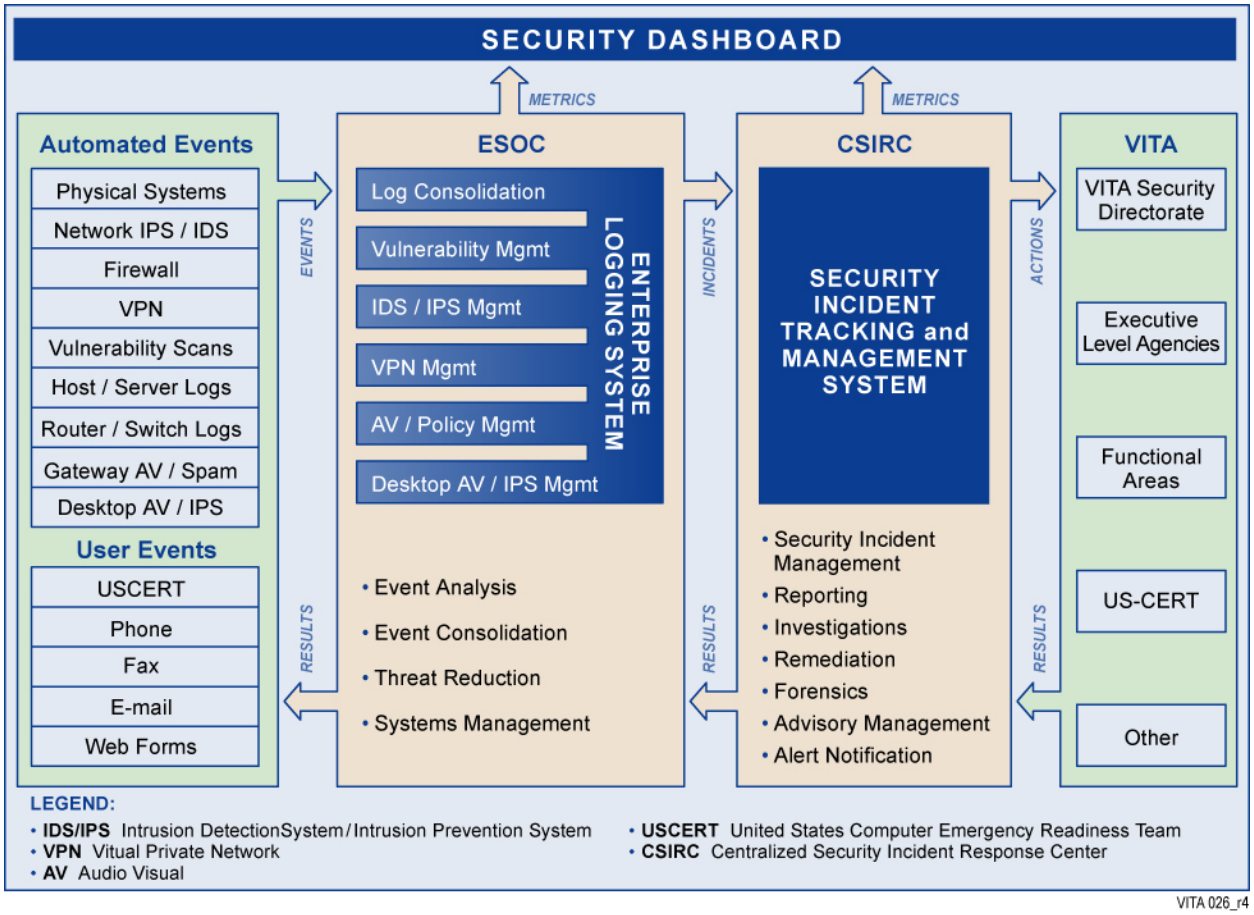

Exhibit 1 VITA IT Security Workflow

Enterprise Security Operations Center

Northrop Grumman will collocate the ESOC with the Southwest Enterprise Solutions Center as a component of the Northrop Grumman CMOC. The CSIRC will be collocated with the Richmond Enterprise Solutions Center. The ESOC and CSIRC system equipment are completely redundant with a separation of over 100 miles between the centers. Security systems monitor entry into the Richmond Enterprise Solutions Center CSIRC and the Southwest Enterprise Solutions Center ESOC facilities; Radio Frequency Identification (RFID) badge reader allows access. The CSIRC and ESOC access are protected additionally by a biometric/card reader combination. This will provide appropriate security staff and leadership has access to the security systems and data within, as well as being protected by the initial defense layer at the building entrance. Further, audit records are available to track who enters and exits.

The ESOC focuses its 24x7 effort on real-time, proactive monitoring, assessing and analyzing the security posture of the VITA Enterprise. Defense of the Commonwealth includes all activities classified as security events, eventually becoming categorized as a threat or non-threat. Upon the determination of active incident status, the ESOC elevates the information to the CSIRC for action and tracking. The two teams of personnel will be cross-trained on ESOC and CSIRC duties, stationed at the separate locations but working in parallel and with separate responsibilities. The ESOC staff will monitor, manage, and maintain all security-related technologies including antivirus, firewalls, IDS/IPS, content filtering, network scanning, and identification management capabilities. They will assist VITA in the creation and maintenance of the VITA Security Plan, a detailed account of the IT security efforts within the enterprise with emphasis on the configuration management, change control, risk assessment, and vulnerability assessment plans.

The ESOC shall contribute to VITA IT security awareness by monitoring, assessing, responding, and managing security operations for the VITA Enterprise.

IT Security Awareness Training

Northrop Grumman will conduct IT security awareness training a minimum of once per year through the VSP, on an as-needed basis through e-mail for immediate-need enterprise training, and when security events deem it necessary.

Training records will be maintained, and the requirement versus completion metrics is used as input into the VITA Security Dashboard.

Security Policy Focus

Northrop Grumman's ESOC/CSIRC security analysts and leadership will assist VITA in recommending, implementing and reviewing security policy within the VITA framework. This will include formulating draft policies, procedures and guides and ensuring the entry into the approval cycle. Policies will be based on the applicable criteria for the particular business function within the organization, with a focus on controls associated within a management, technical and operational perspective. Northrop Grumman will provide the following security policy development cycle strategy:

- Assist VITA and executive branch agencies in a security policy enhancement service by conducting an initial review of internal VITA policy concerning enterprise-wide security
- Assist VITA and executive branch agencies in providing solutions and mechanisms to adhere to Commonwealth of Virginia mandates
- Assist VITA and executive branch agencies in the policy compliance and enforcement arena by focusing on the following areas:
  - Vulnerability/risk assessments
  - Validation and status metrics
  - Physical security controls
  - Logical security controls
- Enable VITA to conform to all statements defined within the existing security policy and develop a plan to reward compliance and eliminate deficiencies
- Develop periodic working groups comprised of VITA and Northrop Grumman personnel to determine an approach to organizational security controls, which will be reflected in the policy
- Develop the VITA Security Plan in compliance with VITA security policy

Northrop Grumman will assist VITA in the upkeep, review, recommendation, and augmentation of VITA Enterprise policies, while its security system architecture provides the enforcement tool to facilitate compliance.

Physical Security

Both VITA data center locations (Richmond Enterprise Solutions Center and Southwest Enterprise Solutions Center) will use Northrop Grumman physical security techniques.

The physical security will input data into the ESOC in the form of logs that can be audited, as well as input data into the SITMS, where incidents are tracked and managed by the CSIRC**.**

Enterprise Logging System

The ELS is a comprehensive, scalable COTS system with a distributed architecture of Security Information Management System (SIMS) devices that consolidate data from network devices. The system is vendor agnostic, compatible with virtually any system capable of generating log output. The notional system depicted in **Exhibit 2** is a centralized repository or warehouse of the time sequenced data, in which the appliance conducts analysis, correlation and consolidation, leading to security incident response capabilities by sending incident data to the SITMS, as well as providing report generation and VITA Security Dashboard metrics.

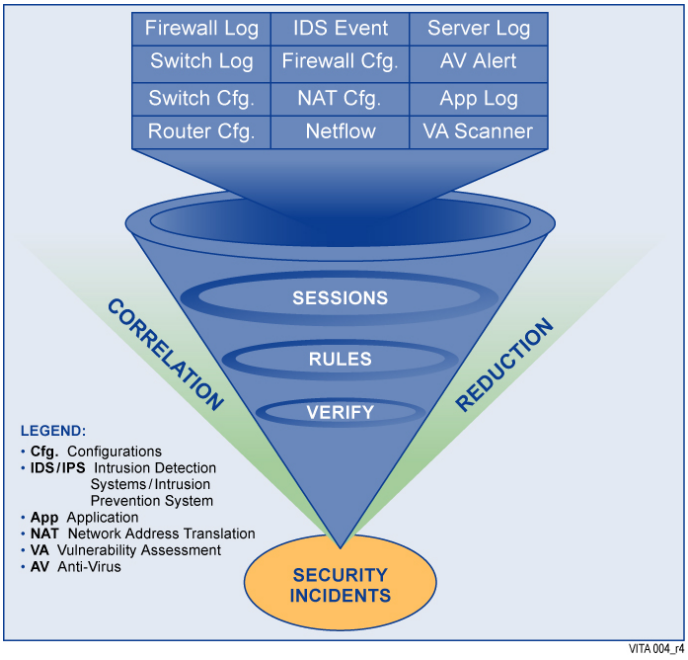

Exhibit 2 Enterprise Logging System

Centralized Security Incident Response Center

The CSIRC is collocated with the Richmond Enterprise Solutions Center and is responsible for all security incidents 24x7. The CSIRC will help VITA and executive branch agencies to comply with **Code of Virginia § 2.2-603.G.** They track, support and maintain user or machine reported incidents by entering the data into the SITMS.

The CSIRC staff is responsible for keeping abreast of all advisories from industry, such as US-CERT, as well as investigating security incidents, focusing on sequence, source and time of events. The CSIRC staff will also maintain industry connections, which enables evaluation of global threat conditions with detailed analyses tailored for VITA needs. In addition to reviewing industry information, they review audit logs and reports and conduct forensic operations when necessary. The outcome of their response generates bulletins to be used by VITA Leadership, system administrators, Information Security System Officers (ISSOs) and network administrators. The bulletins contain status, remediation or recommended actions for the security incident, as well as mitigation plans to prevent future occurrence of events. The bulletins are displayed within the VITA Enterprise Dashboard and provide the ability to perform compliance reporting on bulletin remediation status.

The CSIRC is staffed by dual-trained personnel with capabilities of operating both CSIRC and ESOC systems. Those operations are detailed in standard operating procedures, and the staff is required to attend internal refresher training on both CSIRC and ESOC responsibilities.

Security Incident Tracking and Management System

The CSIRC personnel use the SITMS to track and manage security incidents within the VITA Enterprise. It is a single repository of all VITA and executive-level agency security incident data,

to be used for security incident management and remediation tracking from both machine and user-generated incidents.

The SITMS database resides on the security storage area network (SAN), which is deployed within the ESOC/CSIRC facilities. Metrics from this data are input into the VITA Security Dashboard, and output to appropriate personnel in report format. The SITMS is the primary producer of data metrics.

Enterprise Vulnerability Assessment System

The Enterprise Vulnerability Assessment System (EVAS) is a COTS-based solution comprised of two subcomponents. The first is a distributed architecture that uses the functionality of existing agents installed on servers and desktops to perform assessments and report deficiencies in known vulnerabilities and compliance to security policy configurations. These assessments provide detailed compliance enforcement information, and are not limited to antivirus compliance, patch level compliance, presence of unknown hardware/software, and firewall status. This information is relayed to the patch management platform, where actions generate automatic patch or configuration update and report generation.

Enterprise Identity Management Solution

Northrop Grumman will provide an Enterprise Identity Management Solution (EIMS) through a combination of the physical identity credentialing for Richmond Enterprise Solutions Center/Southwest Enterprise Solutions Center access and Active Directory.

Enterprise Intrusion Detection/Intrusion Prevention System

The EID/IPS provides a standard, proven architecture for monitoring VITA and enterprise-level agencies network, desktops and servers for intrusion prevention and detection capabilities using COTS-based products that provide signature and anomaly-based intrusion recognition. The system is deployed in a tiered architecture, providing defense-in-depth using desktop, host (HIDS/HIPS) and network (NIDS/ NIPS) sensors. The security event information is stored online for 45 days at a minimum, or as dictated by VITA policy. Management of the appliances is securely conducted at ESOC primarily and CSIRC secondarily through the use of approved encryption mechanisms, depending on scheduled maintenance, planned or imminent disaster recovery.

Enterprise Firewall Management System

The Enterprise Firewall Management System (EFMS) will be a standardized management console and configuration repository for the firewalls deployed throughout the VITA Enterprise. The system will deploy VITA-approved configuration changes, store the time stamped configuration in the SAN, and perform firewall monitoring, updates and patches. This system shall provide a high availability by storage of the configurations and ease of deployment in case of firewall failure. The system is the primary change and configuration management process. The VITA Enterprise firewalls will be configured to feed log data into the ELS, becoming metrics within the VITA Security Dashboard.

VITA Security Dashboard

The VITA Security Dashboard is a Web-accessible metric reporting capability provided as a component of the Northrop Grumman VSP. The system is comprised of COTS-based products specifically tailored for VITA, and will provide report generation and print capabilities when needed.

Security Engineering

Northrop Grumman's security engineering provides VITA with a resource pool of qualified individuals to support and make recommendations for security policy, as well as logical and physical access controls. The security engineering team will provide up-to-date information on security trends as well as products to meet an evolving threat environment.